

УДК: 342.9(045)

DOI: <https://doi.org/10.32366/2523-4269-2019-69-4-183-189>



Пересада Ольга Михайлівна,

кандидат юридичних наук

(Донецький юридичний інститут МВС України,
м. Маріуполь)

ORCID: <https://orcid.org/0000-0001-7199-1938>

РОЛЬ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ В ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ: ТЕОРЕТИКО- МЕТОДОЛОГІЧНІ АСПЕКТИ

Статтю присвячено дослідженню теоретико-методологічних аспектів місця та ролі Національної поліції в забезпеченні інформаційної безпеки держави. Проаналізовано функції та повноваження органів поліції у сфері забезпечення інформаційної безпеки суспільства та держави. На підставі проведеного аналізу систематизовано форми, методи та практичні аспекти діяльності кіберполіції в сучасних умовах розвитку інформаційних технологій та розбудови інформаційного суспільства. Наголошується, що побудова європейської моделі організації та діяльності Національної поліції є важливим напрямком діяльності держави та актуальним аспектом забезпечення її інформаційної безпеки в сучасних умовах європейської міждержавної інтеграції та імплементації до українського законодавства європейських правових стандартів інституціонального та інструментального юридичного змісту.

Ключові слова: Національна поліція України; правоохоронна система; правоохоронна діяльність; кіберполіція; інформаційна безпека; національна безпека; інформаційна загроза.

Актуальність дослідження. У сучасних умовах появи принципово нових інформаційних загроз національній безпеці держави, прогресивного розвитку інформаційно-комунікаційних технологій, перманентної появи нових форм та засобів як внутрішнього, так і зовнішнього інформаційного впливу значно актуалізується та об'єктивується інституціональна роль правоохоронних органів, зокрема поліції, у реалізації державної стратегії подолання та запобігання таким загрозам та викликам.

Окреслене завдання Національної поліції України набуває особливого значення та змісту в наявних умовах комплексної агресії Російської Федерації проти державного суверенітету, територіальної цілісності, політичної незалежності нашої держави, однією зі складових якої є саме інформаційна агресія, що полягає, по-перше, у спланованій систематичній інформаційній пропаганді ЗМІ, інтернет-ресурсів, соціальних мереж; по-друге, у військово-технічному шпіонажі з використанням електронних технологій; по-третє, у прямих кібератаках на об'єкти економічної та управлінської інфраструктури тощо.

У подібних умовах пріоритетним завданням держави є створення ефективної правоохоронної системи, здатної протистояти вказаним викликам та загрозам, і забезпечення її належного функціонування. Зі свого боку, ключову роль у забезпеченні інформаційної безпеки суспільства й держави в умовах функціонування європейської моделі правоохоронної системи відіграють саме органи поліції, що й визначає важливість теоретико-

методологічного та науково-практичного завдання, яке вирішується в наданому дослідженні.

Аналіз останніх досліджень і публікацій. Проблематика забезпечення інформаційної безпеки суб'єктами публічної влади різного рівня, а також визначення інституціонального місця та ролі органів поліції на сучасному етапі їхньої модернізації ретельно розглядається у вітчизняній юридичній літературі. Зокрема можна відзначити праці В. Б. Авер'янова, О. М. Бандурки, В. М. Бесчастного, С. А. Вавренюка, Ю. О. Винокурова, В. Д. Гавловського, В. А. Глуховері, В. О. Голубева, Р. А. Калюжного, А. Т. Комзюка, М. І. Корнієнка, Н. В. Лесько, В. Я. Малиновського, Р. М. Пилипіва, О. С. Проневич, В. С. Цимбалюка, В. М. Циндрі, О. Н. Ярмиша та інших дослідників.

Водночас ще не вироблено концептуальні підходи до ролі органів поліції в реалізації функції забезпечення інформаційної безпеки держави на тлі інтенсифікації впровадження європейських стандартів організації та діяльності органів внутрішніх справ, формування новітньої теоретичної моделі державної інформаційної політики, побудови дієвого механізму реалізації поліцейської реформи в Україні. Ретельної розробки, зокрема, потребують форми та методи діяльності органів поліції в комплексному забезпеченні інформаційної безпеки як одного з найважливіших телеологічних напрямів гарантування національної безпеки держави загалом.

Мета статті – дослідити інституціональні теоретико-методологічні аспекти діяльності Національної поліції України стосовно забезпечення інформаційної безпеки держави.

Виклад основного матеріалу. Розглядаючи інституціональні теоретико-методологічні аспекти забезпечення інформаційної безпеки держави, слід зазначити, що відповідно до ст. 2 Закону України «Про Національну поліцію» від 02.07.2015, «завданнями поліції є надання поліцейських послуг у сферах: 1) забезпечення публічної безпеки і порядку; 2) охорони прав і свобод людини, а також інтересів суспільства і держави; 3) протидії злочинності; 4) надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги» [1].

Виходячи з аналізу положень цієї норми профільного закону, ключовим для формування належного розуміння місця та ролі Національної поліції в забезпеченні інформаційної безпеки вважаємо завдання стосовно забезпечення «охорони прав і свобод людини, а також інтересів суспільства і держави» (п. 2 ст. 2), адже інформаційна безпека становить важливий структурний елемент національної безпеки та національних інтересів держави й суспільства взагалі.

У цьому контексті слід зазначити, що загалом сформувався два доктринальних підходи до визначення поняття «національна безпека». Згідно з першим, національна безпека розглядається у вимірі національних інтересів (інакше кажучи, ідеться якраз про «інтереси суспільства і держави», через які етимологічно формулюється одне з інституціональних завдань Національної поліції України. – Авт.), а згідно із другим, – у концептуальній парадигмі базисних цінностей суспільства (у розумінні громадянського суспільства, автономного від державних інтересів у вузькому тлумаченні цієї політико-правової категорії. – Авт.) [2, с. 26–27].

Як слушно вказує Г. П. Ситник, на етапі формування відповідного лексикону поняття «національна безпека» використовувалося передусім як синонім до дефініції «обороздатність держави», тобто у значенні виключно політичної та воєнної безпеки [2, с. 27].

Водночас із подальшим розвитком уявлень про змістовне наповнення цієї категорії актуальним стало її комплексне, різнобічне розуміння. Так, на думку А. В. Возженікова, національна безпека як соціальне явище має багато відтінків, закріплених правом як сукупний стан, який акумулює безкінечну множину видів збитків, а також можливих уявлень про загрози та їхні наслідки, а тому національну безпеку слід розглядати як «...стан краї-

ни, за якого відсутні або усунені...реальні зовнішні та внутрішні загрози її національним цінностям, інтересам і національному способу життя, тобто забезпечується реалізація життєво важливих інтересів особи, суспільства й держави» [3, с. 55].

Сучасні тлумачні словники трактують поняття «безпека» як стан, коли немає небезпеки, тобто як стан, за якого ніщо не загрожує кому-небудь або чому-небудь [4, с. 84]. З подібним визначенням не можна погодитися повністю, адже за такого підходу розглядається виключно ідеальна ситуація, що навряд чи може бути досягнута за реальних політичних, правових, соціально-економічних, культурних (духовних) умов існування будь-якого сучасного суспільства та світу загалом. Найімовірніше, у цьому контексті варто визнати справедливим зауваження В. Л. Манілова про те, що зміст категорії «безпека» складає певний стан системи, досягнутий внаслідок запобігання шкоди її розвитку (життєдіяльності) [5, с. 29].

Крім того, на користь такого підходу до визначення юридичної сутності терміна «безпека» свідчить зміст міжнародно-правових документів, найперше – Статуту ООН, який визначив як одну з головних цілей створення та діяльності ООН об'єднання зусиль міжнародного співтовариства для підтримання безпеки, а держави-учасниці ОБСЄ у ст. 5 Заключного акта від 1 серпня 1975 р. визначили «...утримуватися від будь-яких дій, які можуть погіршити становище до такої міри, що буде поставлено під загрозу підтримання...безпеки» [6, с. 9]. Отже, на міжнародно-правовому рівні під безпекою в широкому значенні розуміється певна якість міжнародних відносин, що ставиться в залежність від того чи іншого рівня міждержавних правовідносин, а тому безпеку можна розглядати як своєрідну інтегральну характеристику соціальної системи, яка залежить від багатьох параметрів і характеризує той чи інший її стан (аж до людської цивілізації включно). У цьому разі досягнення такого стану соціальної системи визначає її головну ціль, а також спосіб та умови існування під впливом тих чи інших факторів [2, с. 22].

Зі свого боку, інформаційна безпека в сучасних умовах розвитку інформаційно-комунікаційних технологій є однією з ключових складових національної безпеки держави, зважаючи на характер наявних інформаційних загроз та викликів життєво важливим суспільним і державним інтересам.

Необхідно відзначити, що поняття «інформаційне суспільство» є новітнім для науково-доктринального термінологічного обігу. При цьому в науковій літературі спостерігається деяка розбіжність у думках про авторство цього поняття. Так, на погляд одних дослідників, у науковий обіг поняття «інформаційне суспільство» увійшло наприкінці 60-х – початку 70-х років ХХ ст. Його автором став Ю. Хаяші, але водночас у розробленні цього поняття брали активну участь також організації, що працювали на японський уряд, поміж них: Агентство економічного планування, Інститут розробки й використання комп'ютерів, Рада зі структури промисловості. Зі звітів цих організацій за 1969–1971 рр. стає зрозумілим, що інформаційне суспільство – це суспільство, у якому процес комп'ютеризації дає людям доступ до надійних джерел інформації, рятує їх від рутинної роботи, забезпечує високий рівень автоматизації виробництва. Як вважають автори нової концепції, «... виробництво інформаційного продукту, а не продукту матеріального, буде рушійною силою утворення і розвитку суспільства» [7, с. 29].

На думку інших учених, зокрема В. Іноземцева, термін «інформаційне суспільство» був уведений у науковий обіг на початку 60-х років ХХ ст. фактично одночасно у США і Японії Ф. Махлупом і Т. Умесао. Так було започатковано теорію, яка була розвинута такими відомими авторами, як М. Порат, Й. Масуда, Т. Стоуньєр, Р. Катц та ін. До напрямку, що розглядає еволюцію людства крізь призму прогресу знання, прилучаються і деякі інші теорії, наприклад концепція технотронного суспільства, створена З. Бжезинським, а також теорії, що підкреслюють вирішальну роль знань у життєдіяльності сучасного соціуму (англ. »the knowledgeable society», «knowledge society», «knowledge-value society») [8, с. 21].

Подібне значення інформації, інформаційного обміну та інформаційних технологій у життєдіяльності сучасного суспільства об'єктивує важливість забезпечення інформаційної безпеки суспільства й держави як стану захищеності життєво важливих суспільних і державних інтересів від різноманітних інформаційних загроз.

Специфічною особливістю забезпечення інформаційної безпеки держави як поліцейської функції є необхідність охорони та захисту інформації в соціотехнічних системах, що викликає доцільність застосування спеціальних знань із технічних галузей, підгалузей, окремих інституцій як технічних, так і суспільних наук, а сама інформаційна безпека за природою походження в умовах інформаційного суспільства має триєдиний зміст: організаційний, інженерно-технічний (у тому числі програмно-технічний) та правовий [9, с. 248–249].

Таким чином, сутність завдань поліції як суб'єкта забезпечення інформаційної безпеки держави визначається провідним предметом суспільних відносин у вказаній сфері, яким є інформація в автоматизованих (комп'ютерних) системах, у тому числі в електронних телекомунікаціях, зокрема в мережі Інтернет [9, с. 249].

Особливості вирішення вказаних завдань із застосуванням цілісного комплексу як соціогуманітарних, так і технічних знань зумовили необхідність створення спеціального підрозділу Національної поліції України – Департаменту кіберполіції як міжрегіонального територіального органу Національної поліції зі статусом юридичної особи публічного права [10].

Метою створення кіберполіції в Україні було реформування та розвиток підрозділів МВС України, що забезпечило підготовку та функціонування висококваліфікованих фахівців в експертних, оперативних та слідчих підрозділах поліції, задіяних у протидії кіберзлочинності, та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності.

Міністр внутрішніх справ України А. Б. Аваков після утворення вказаного підрозділу цілком слушно визначив такі основні завдання кіберполіції, як:

1. Реалізація державної політики у сфері протидії кіберзлочинності.
2. Завчасне інформування населення про появу новітніх кіберзлочинів.
3. Упровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини.
4. Реагування на запити закордонних партнерів, що надходять каналами Національної цілодобової мережі контактних пунктів.
5. Участь у підвищенні кваліфікації працівників поліції стосовно застосування комп'ютерних технологій у протидії злочинності.
6. Участь у міжнародних операціях та співпраця в режимі реального часу. Забезпечення діяльності завдяки мережі контактних пунктів між 90 країнами світу.
7. Протидія кіберзлочинам, а саме:

- у сфері використання платіжних систем: скімінг (шимінг) – незаконне копіювання вмісту треків магнітної смуги (чипів) банківських карток; кеш-трепінг – викрадення готівки з банкомата шляхом устанавлення на шатер банкомата спеціальної накладки-утримувача; кардинг – незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджені її власником; несанкціоноване списання коштів із банківських рахунків за допомогою систем дистанційного банківського обслуговування;

- у сфері електронної комерції та господарської діяльності: фітінг – виманювання в користувачів Інтернету їхніх логінів та паролів до електронних гаманців, сервісів онлайн-аукціонів, переказування або обміну валюти тощо; онлайн-шахрайство – заволодіння коштами громадян через інтернет-магазини, сайти та телекомунікаційні засоби зв'язку;

- у сфері інтелектуальної власності: піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті; кардшарінг – надання незаконного доступу до перегляду супутникового та кабельного телебачення;

- у сфері інформаційної безпеки: соціальна інженерія – технологія управління людьми в Інтернет-просторі; шкідливе програмне забезпечення (англ. «malware») – створення та розповсюдження вірусів і шкідливого програмного забезпечення; протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості й насильства; рефайлінг – незаконна підміна телефонного трафіка.

Аналізуючи окреслені завдання, у сучасних умовах прогресивного інформаційно-комунікаційного розвитку загалом зазначимо такі ключові концептуальні напрями забезпечення інформаційної безпеки, як завдання Національної поліції України:

1. Організація протидії не бажаному для інтересів суспільства й держави впливу за допомогою технічних засобів захисту, причому засоби захисту мають бути адекватними засобам впливу, що означає необхідність застосування належних за кількістю та якістю технічних засобів захисту інформаційних систем (наприклад, створення системи просторового зашумлення для приховування інформації в обмеженому середовищі чи екранування технічних засобів у приміщенні).

2. Організація протидії негативному впливу на учасників інформаційних відносин, зокрема протидія кіберзлочинам як таким, що несуть безпосередню суспільну небезпеку.

3. Визначення майнових і моральних утрат та їхня мінімізація в разі порушення функціонування інформаційної системи, важливої для належного забезпечення інтересів суспільства та держави, включаючи взаємодію з іншими правоохоронними та судовими органами як України, так і зарубіжних держав для притягнення до відповідальності й відшкодування заподіяних протиправними діями (бездіяльністю) збитків.

Отже, заходи у сфері забезпечення інформаційної безпеки держави, що здійснюють органи поліції, з теоретико-методологічних позицій можна класифікувати на такі види, як: 1) організація запобіжних заходів; 2) організація блокування (протидії) реальних інформаційних загроз; 3) організація подолання наслідків інформаційних загроз, якщо їм не вдалося запобігти.

Висновки. Таким чином, під час аналізу теоретико-методологічних аспектів місця та ролі Національної поліції в забезпеченні інформаційної безпеки держави можна дійти загальних висновків, а саме: а) у сучасних умовах розвитку інформаційного суспільства та науково-технічного прогресу інформаційна безпека є ключовим структурним елементом національної безпеки як стану достатньої захищеності життєво важливих суспільних і державних інтересів; б) забезпечення інформаційної безпеки на сучасному етапі потребує комплексного застосування як гуманітарних, так і спеціальних технічних знань, що об'єктивує створення окремого підрозділу (Департаменту кіберполіції) у структурі Національної поліції України; в) ключовими концептуальними напрямами забезпечення інформаційної безпеки органами поліції є організація протидії не бажаному для інтересів суспільства та держави впливу за допомогою технічних засобів захисту; організація протидії негативному впливу на учасників інформаційних відносин, зокрема протидія кіберзлочинам як таким, що несуть безпосередню суспільну небезпеку; визначення майнових і моральних утрат та їхня мінімізація в разі порушення функціонування інформаційної системи; г) заходи у сфері забезпечення інформаційної безпеки держави, що здійснюють органи поліції, з теоретико-методологічних позицій можна класифікувати на такі види: організація запобіжних заходів; організація блокування (протидії) реальних інформаційних загроз; організація подолання наслідків інформаційних загроз, якщо їм не вдалося запобігти; д) ключовим завданням Національної поліції вбачається завчасна профілактика та запобігання правопорушенням в інформаційному середовищі суспільної життєдіяльності.

Список використаних джерел

1. Про Національну поліцію : закон України від 02 липня 2015 р. *Відомості Верховної Ради України*. 2015. № 40–41. Ст. 379.
2. Національна безпека України : навч. посібник / Ситник Г. П. та ін.; за заг. ред. Г. П. Ситника. Київ : Кондор, 2007. 616 с.
3. Возжеников А. В. Национальная безопасность (теория, политика, стратегия) : монография. Москва : НПО Модуль, 2000. 240 с.
4. Ващенко Л. О., Єфімов О. М. Тлумачний словник – мінімум української мови. Київ : Довіра, 2000. Вид. 2-ге. 546 с.
5. Манилов В. Л. Безопасность в эпоху партнёрства : монография. Москва : ТЕРРА, 1999. 368 с.
6. Ведомости Верховного Совета СССР. Москва. 1975. С. 7–10.
7. Правова інформатика : підручник. У 2 т. Київ : Парлам. вид-во, 2004. Т. 1. 416 с.
8. Бжезинский З. Великая шахматная доска. Господство Америки и его геостратегические императивы : монография. Москва : Междунар. отношения, 1999. 256 с.
9. Основи інформаційного права України : навч. посіб. / В. С. Цимбалюк та ін.; за ред. М. Я. Швеця. Київ : Знання, 2009. Вид. 2-ге, переробл. і допов. 414 с.
10. Про утворення територіального органу Національної поліції : Постанова Кабінету Міністрів України від 13 жовтня 2015 р. № 831. URL : <https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF> (дата звернення: 20.11.2019).

Пересада Ольга Михайловна,

кандидат юридических наук

(Донецкий юридический институт МВД Украины, г. Мариуполь)

ORCID: <https://orcid.org/0000-0001-7199-1938>

РОЛЬ НАЦИОНАЛЬНОЙ ПОЛИЦИИ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА: ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ

Статья посвящена исследованию теоретико-методологических аспектов места и роли Национальной полиции в обеспечении информационной безопасности государства. Проанализированы функции и полномочия органов полиции в сфере обеспечения информационной безопасности общества и государства. На основании проведённого анализа систематизированы формы, методы и практические аспекты деятельности киберполиции в современных условиях развития информационных технологий и развития информационного общества. Отмечается, что построение европейской модели организации и деятельности Национальной полиции является важным направлением деятельности государства и актуальным аспектом обеспечения его информационной безопасности в современных условиях европейской межгосударственной интеграции и имплементации в украинское законодательство европейских правовых стандартов институционального и инструментального юридического содержания.

Ключевые слова: Национальная полиция Украины; правоохранительная система; правоохранительная деятельность; киберполиция; информационная безопасность; национальная безопасность; информационная угроза.

Peresada Olga,

PhD in Law

(Donetsk Law Institute, MIA of Ukraine, Mariupol)

ORCID: <https://orcid.org/0000-0001-7199-1938>

THE ROLE OF THE NATIONAL POLICE OF UKRAINE IN ENSURING THE INFORMATION SECURITY OF THE STATE: THEORETICAL AND METHODOLOGICAL ASPECTS

The article is devoted to the study of theoretical and methodological aspects of the place and role of the National Police in ensuring the information security of the state. The functions and powers of the police in the field of information security of society and the state are analyzed. Based on the analysis, the forms, methods and practical aspects of the activities of cyber police in the current conditions of the development of information technology and the development of the information society are analyzed and systematized. It is noted that the structure of a European model of the organization and activities of the National Police is an important direction of the state's activity and an urgent aspect of ensuring its information security in modern conditions of European interstate integration as well as the implementation of European legal standards of institutional and instrumental legal content in Ukrainian legislation. Thus, by analyzing the

theoretical and methodological aspects of the place and role of the National Police in the provision of information security of the state, we can come to the following general conclusions: a) protection of vital public and state interests and provision of information security at the present stage requires a comprehensive application of both humanitarian and specialized technical knowledge, which obstructs the creation of a separate unit (Department of Cyber Police) within the structure of the National Police of Ukraine; c) the key conceptual directions of ensuring information security by the police are: organization of counteracting for undesirable actions for the interests of society and the state by means of modern technologies; organization of counteraction to the negative impact on participants of information relations, including counteraction to cybercrimes that cause immediate public danger; determination of property and moral losses and their minimization in case of disruption of the information system functioning; d) measures of providing information state security, carried out by the police, from the theoretical and methodological standpoints can be classified into the following types: organization of preventive measures; organization of blocking (counteraction) to real information threats; organization of overcoming the consequences of information threats, if they could not be prevented; e) the key task of the National Police is the early prevention as well as the prevention of offenses in the information environment of public life.

Key words: National Police of Ukraine; law enforcement system; law enforcement; cyber police; information security; national security; information threat.

Надійшла до редколегії 03.12.2019